

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-256144

(P2003-256144A)

(43) 公開日 平成15年9月10日 (2003.9.10)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 3/06	3 0 1	G 0 6 F 3/06	3 0 1 M 5 B 0 6 5
	3 0 4		3 0 4 H 5 B 0 8 2
12/00	5 4 5	12/00	5 4 5 A 5 B 0 8 9
13/00	3 5 1	13/00	3 5 1 B

審査請求 未請求 請求項の数10 O L (全 19 頁)

(21) 出願番号 特願2002-52620 (P2002-52620)

(22) 出願日 平成14年2月28日 (2002.2.28)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 加納 義樹

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 北村 学

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100075096

弁理士 作田 康夫

最終頁に続く

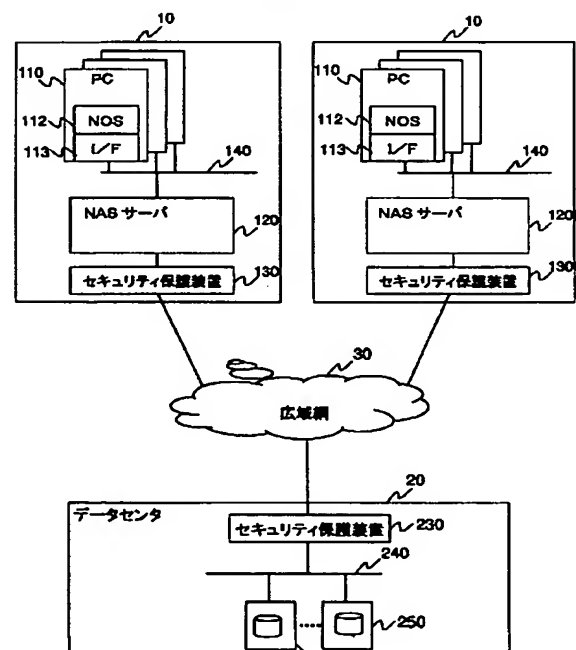
(54) 【発明の名称】 記憶装置

(57) 【要約】

【課題】 ユーザがデータの保管場所を意識することなく安全にファイルにアクセスできる手段を提供する。

【解決手段】 1または複数台の計算機110とLAN140を介して接続され、これら計算機からファイルデータのアクセス要求を受け付けるサーバ装置120と、サーバ装置120と広域網30を介して接続され、ファイルデータを記憶する記憶装置250が設けられる。計算機110とサーバ装置120との間の通信は、ネットワークファイルプロトコルを用いて行われ、サーバ装置と記憶装置との間の通信は、ブロックデバイスプロトコルを用いて行われる。サーバ装置120及び記憶装置250は、それぞれ、セキュリティ装置130、230を介して広域網に接続される。

図1



【特許請求の範囲】

【請求項１】記憶装置と、

前記記憶装置に格納されるファイルデータの格納場所、及びアクセス状態を管理する管理情報を保持する管理サーバと、

ネットワークを介して計算機より第１のプロトコルでファイルデータのアクセス要求を受け付け、前記管理情報に基づいて前記計算機からアクセス要求に応じ、第２のプロトコルで前記記憶装置へのアクセスを行うサーバ装置とを有することを特徴とする記憶装置システム。

【請求項２】前記第１のプロトコルは、ネットワークファイルアクセスプロトコルであって、前記第２のプロトコルはブロックデバイスプロトコルであることを特徴とする請求項１記載の記憶装置システム。

【請求項３】前記ブロックデバイスプロトコルとしてｉＳＣＳＩを用いたことを特徴とする請求項２記載の記憶装置システム。

【請求項４】前記サーバ装置と、前記記憶装置とは、セキュリティ保護装置を介して接続されることを特徴とする請求項２記載の記憶装置システム。

【請求項５】データを記憶する第１の記憶装置と、データを記憶する第２の記憶装置と、前記第１の記憶装置とローカルに接続され、前記第２の記憶装置と広域網を介して接続されるサーバ装置であって、ローカルなネットワークを介して計算機よりファイルデータのアクセス要求を受け付け、該アクセス要求によりアクセスすべきデータが前記第１及び第２の記憶装置のいずれに格納されているかを判別し、該判別の結果に応じて前記第１の記憶装置、または前記第２の記憶装置へのアクセスを行うサーバ装置とを有する記憶装置システム。

【請求項６】前記サーバ装置とネットワークを介して接続され、前記第２の記憶装置に格納されるデータの格納位置、及びアクセス状態を管理するための情報を保持する管理サーバを有することを特徴とする請求項５記載の記憶装置システム。

【請求項７】前記サーバ装置は、前記第２の記憶装置に格納されたデータをアクセスする際、前記管理サーバにアクセス要求を発行し、該アクセス要求に対する応答に基づいて前記第２の記憶装置をアクセスすることを特徴とする請求項６記載の記憶装置システム。

【請求項８】前記サーバ装置は、セキュリティ保護装置を介して前記第２の記憶装置と接続されることを特徴とする請求項５記載の記憶装置システム。

【請求項９】前記サーバ装置を複数備え、前記第２の記憶装置には、該複数のサーバ装置により共用されるデータが格納されることを特徴とする請求項６記載の記憶装置システム。

【請求項１０】データを記憶する記憶装置と、

あって、ローカルなネットワークを介して計算機よりネットワークファイルプロトコルを用いたファイルデータへのアクセス要求を受け付け、該アクセス要求に応答して、前記記憶装置に格納されたファイルデータをブロックデバイスプロトコルを用いてアクセスするサーバ装置とを有することを特徴とする記憶装置システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、計算機により利用されるデータを管理する記憶装置システムに係り、特に、広域網を介してデータを管理することの可能な記憶装置システムとそのファイルの保管、管理方法に関する。

【０００２】

【従来の技術】近年、情報化の進展により、企業等で作成されるデータは、飛躍的に増えてきている。例えば、企業内においては、各部署でデータが作成されるため、必然的にデータの管理も各部署で行われている。企業におけるデータ管理の一例として、作成されたデータのバックアップがある。バックアップでは、例えば、磁気ディスク装置に格納されている業務上重要な情報（データ）が、磁気ディスク装置からテープデバイス等の二次記憶装置にコピーされる。バックアップの頻度も、データの増大に伴い増大している。

【０００３】このようなデータの管理を集約的に管理することにより、データの管理を一元的に行うことができ、企業でのデータ管理に要するコストの削減が可能になる。例えば、データが各部署に分散されており、各部署で日々バックアップを行うより、情報を集約化し、一元化して管理を行う方が効率的であって望ましい。

【０００４】情報の一元化に適した装置として、ＲＡＩＤに代表されるような高信頼な大容量記憶装置がある。ＲＡＩＤでは、数テラバイトの記憶領域を複数の小さな論理的な記憶領域に分けることで、集約的に小さなグループごとの情報を１つにまとめることができる。このようなＲＡＩＤの特徴を生かして、企業内の各部署で分散して管理されていたデータが、情報部門内の大型計算機センタ等において、一元的に管理されるようになってきた。

【０００５】このようなデータの一元管理の流れは、企業内にとどまらない。最近では、データセンタにおいて、複数の企業のデータを受託管理するサービス業者が現れ始めている。データセンタでは、複数の企業のデータを安全にかつ迅速に管理することが求められており、情報をより容易に管理する手段が必要とされている。しかし、ＲＡＩＤでは、記憶領域をブロック単位としてデータが取り扱われるため、データセンタの管理者にとってその管理が難しい。

【０００６】一方で、ブロック単位での管理の難しさを

て、Network Attached Storage（略してNAS）と呼ばれるファイルサーバがある。NASでは、パーソナルコンピュータ（PC）やワークステーションが備えるNFS（Network File System）やCIFS（Common Internet File system）等のネットワークファイルプロトコルを用いたアクセスが可能である。このため、データ管理をファイル単位で行うことができ、ブロック単位での管理と比べてデータの管理が容易である。

【0007】

【発明が解決しようとする課題】NASで取り扱われるネットワークファイルプロトコルは、ローカルエリアネットワーク（LAN）を前提にして作られている。このため、ネットワークとして広域網を適用すると、距離によるアクセスの遅延のためファイルへの安定したアクセスが行えず、結果としてデータの破壊を招く可能性がある。したがって、企業がNASを導入した場合、記憶装置の管理をデータセンタなどの外部に委託することが難しくなる。さらに、企業やデータセンタ等は、広域網からの不正進入を防ぐために、ファイアウォールなどのセキュリティ保護装置を多段に備えつけることが多いため、データセンタでNASを管理したとしても、企業のPCからデータセンタ内のNASへ接続することは非常に難しい。

【0008】本発明の目的は、広域網を介して接続されるNASサーバとデータセンタ間で、安全な論理通信網を構築し、データセンタ内の記憶装置をNASサーバで利用を可能にして、データセンタ内で保管されたデータを複数のNASサーバ間で共有する手段を提供することにある。

【0009】

【課題を解決するための手段】本発明によれば、1または複数台の計算機とLANを介して接続され、これら計算機からファイルデータのアクセス要求を受け付けるサーバ装置と、該サーバ装置と広域網を介して接続され、前記ファイルデータを記憶する記憶装置とを有する。サーバ装置は、計算機からのアクセス要求に応じて、記憶装置に保持されたファイルデータをアクセスする。

【0010】本発明の好ましい態様において、計算機とサーバ装置との間の通信は、ネットワークファイルプロトコルを用いて行われ、サーバ装置と記憶装置との間の通信は、ブロックデバイスプロトコルを用いて行われる。サーバ装置及び記憶装置は、それぞれ、セキュリティ装置を介して広域網に接続される。

【0011】本発明の一つの態様において、サーバ装置は、自身に直接接続される内部記憶装置を備える。サーバ装置は、外部の記憶装置及び内部の記憶装置に記憶されるファイルデータの管理情報を保持し、計算機からのアクセス要求に応じて、アクセスすべきファイルデータの格納位置を判別し、外部記憶装置、あるいは内部記憶

【0012】本発明の他の態様においては、複数のサーバ装置と広域網を介して接続されるサーバ管理装置が設けられる。サーバ管理装置は、複数のサーバ装置により共有される記憶装置を管理するための管理情報を保持し、サーバ装置間での記憶装置の共有状態を管理する。

【0013】管理情報は、記憶装置の共有に先立って管理者により設定される。各サーバ装置は、計算機から他のサーバ装置との間で共有している記憶装置へのアクセス要求を受けると、サーバ管理装置にアクセス許可を求める。サーバ管理装置では、この要求に回答して、要求元のサーバ装置が記憶装置の共有を許可されているか調べ、許可されている場合に、アクセスを許可し、アクセスされるべきファイルデータの記憶位置をサーバ装置に通知する。サーバ装置は、受け取った記憶位置に基づいて対象とされるべきファイルデータをアクセスする。

【0014】

【発明の実施の形態】図1は、本発明が適用された計算機システムの一実施形態における構成を示す簡略なブロック図である。

【0015】本実施形態における計算機システムは、企業内に設けられる計算機システム10と、1又は複数の企業内計算機システム10により利用されるデータの管理を行うデータセンタ20を構成する計算機システムが、広域網30を介して相互に接続された構成を有する。ここで、広域網30とは、インターネットのようなIP網、ATM（Asynchronous Transfer mode）網、公衆網など、複数の利用者が通信路を共有することのできるネットワークをいう。また、一般には、企業内計算機システム10とデータセンタ20とは、物理的、あるいは地理的に離れた場所に設けられる。

【0016】企業内計算機システム10は、複数台のパーソナルコンピュータ（PC）110、NASサーバ120、セキュリティ保護装置130、PC110、NASサーバ120を相互に接続するローカルエリアネットワーク（LAN）140を有しており、セキュリティ保護装置130により広域網30と接続されている。

【0017】各PC110は、ネットワーク接続のためのインタフェース112と、CIFSプロトコルやNFSプロトコルに対応し、ネットワークファイルシステムを利用できるネットワークオペレーティングシステム（NOS）113とを備える。PC110は、その他、CPUやメモリ、入出力装置などを有するが、これらについては、本発明と直接関係するものではなく、図示を省略する。PC110上で実行されるNOS113その他のプログラムは、PC110が有する記憶装置に格納される他、NASサーバ120により提供される記憶領域に格納され、その実行時にPC110のメモリにロードされるように構成されていてもよい。

【0018】NASサーバ120は、PC110に対し

は、NFSやCIFSなどのネットワークファイルシステムを用いNASサーバ120の記憶領域を利用することができる。この記憶領域は、磁気ディスク装置で構成される。

【0019】LAN140と広域網30との間の接続には、幾つかの形態が考えられる。本実施形態では、LAN140と広域網30との接続を、セキュリティ保護装置を介して行っている。セキュリティ保護装置130、230は、広域網30からの不意なアクセスによるシステムへの侵入、破壊を防ぎ、計算機システム10とデータセンタ20との間で転送されるデータの盗聴、改ざんや、なりすましを防いだ通信を可能にする。具体的に、セキュリティ保護装置130は、広域網30からの不特定なアクセスを禁止するために、TCP/IPにおける各サービスへの通信路を示すポートのうち、セキュリティ保護装置130、230間で利用されるポート以外のポートを閉塞し、セキュリティ保護装置間130、230で利用されるポートを用いて暗号化された通信路が用意される。暗号化は、各セキュリティ保護装置で予め設定された暗号鍵、暗号鍵の寿命、認証アルゴリズム、暗号アルゴリズム、及び、相手側セキュリティ保護装置のIPアドレスもしくはホスト名等を含む認証情報を用いて行われる。通信路の暗号化を行うプロトコルの一例としてはIPSecがあり、LANからWANへ接続する装置に備えつけられている。

【0020】計算機システム10のLAN140からデータセンタ20のLAN240へのアクセスが、このように暗号化された通信路（以降、暗号化通信路という）を用いて実施される。また、その逆に、LAN240から広域網30経由でLAN140へアクセスする際にも、セキュリティ保護装置130、230間で作られる暗号化回線が用いられる。

【0021】本実施の形態では、セキュリティ保護装置130がNASサーバ120に直接接続されているが、NASサーバ120がセキュリティ保護装置130を通じて外部と通信するよう構成されていれば、LAN140にセキュリティ保護装置130が接続されていてもよい。

【0022】データセンタ20は、広域網30に接続するセキュリティ保護装置230、NASサーバ120の記憶領域となる1又は複数台の記憶装置250を有する。セキュリティ保護装置230、及び記憶装置250は、相互にLAN240を介して接続される。

【0023】記憶装置250は、データを保管するディスク装置とその制御を行う制御装置を含んで構成され、記憶領域となる論理的な記憶装置であるロジカルユニット（LU）を提供している。LUをNASサーバ120等の装置へ提供するために、記憶装置250は、LAN240を介してネットワーク上にSCSIプロトコルを

【0024】図2は、NASサーバ120の構成を示す機能ブロック図である。NASサーバ120は、プロセッサ220、ネットワークインタフェース211、212及び記憶装置215を含んで構成される。

【0025】NASサーバ120は、ネットワークインタフェース211によりLAN140に、また、ネットワークインタフェース212によりセキュリティ保護装置130に接続される。プロセッサ220は、ネットワークインタフェース211、212を介して行われる通信で取得するデータの発信元を把握し、ファイルへのオペレーション情報を確認して記憶領域への処理を行う。

【0026】プロセッサ220は、ネットワークプロトコル処理部221、ネットワークファイルシステム処理部（ネットワークFS処理部）222、ファイルシステム管理部（FS管理部）223、ブロックデバイスプロトコル処理部224、記憶領域管理部225、セキュリティ部227、設定制御部228、及び設定部229を有する。プロセッサ220の有する各部の機能は、プロセッサ220上でのプログラム処理により実現される。

【0027】ネットワークプロトコル処理部221は、TCP/IPのプロトコルに従った処理を行い、ネットワークインタフェース211、あるいは、212より取得されたデータから発信元を確認し、送信データを保証した通信を行う。

【0028】ネットワークFS処理部222は、PC110よりLAN140経由で転送されるファイルオペレーションを処理し、FS管理部223で管理されるファイルシステムへの操作を行う。ファイルオペレーションの処理では、後述するエクスポート管理表の許可済みのディレクトリに対してのみ、ファイルシステムへの実際の操作を行う。未許可ディレクトリに関してはエラーを戻す。

【0029】ファイルオペレーションは、与えられたディレクトリとファイル情報からファイルの有無を検索する“lookup”、検索したファイルへバイト単位での読み出し操作をする“Read”、そして、同様にファイルへバイト単位で書き出し操作をする“Write”等のオペレーションを含む。このようなファイル操作を行うネットワーク処理部の例として、NFSサーバやCIFSサーバがある。

【0030】FS管理部223は、記憶装置215や記憶装置250から提供されるLUに記録されたファイルシステムの構造を示すスーパーブロック、ファイルを構成するi-node、そして、データとファイルシステム内のディレクトリ情報を記録するブロックに基づいて、ファイルシステムの構成を管理する。スーパーブロックは、ファイルシステムの構造を示すために、ファイルシステム内のi-node数、ブロック数、ブロックの利用可能開始領域の論理ブロックアドレス（LBA）、ファイルシ

む。

【0031】i-nodeは、ファイルシステム中で順序づけて保存されている。i-nodeには、ファイルの保護アクセス権を設定するモード、ファイルの所有者、ファイルサイズ、ファイルへの最終更新時刻、ファイルへのリンク数、アクセス可能なグループ、そして、データが含まれるブロックへのリンクに関する情報が含まれている。ファイルの場合にはブロックの1つにファイル名が記される。ディレクトリの場合には、そのディレクトリの中に存在するすべてのファイル名もしくはディレクトリ名と、その名前に対応するi-node番号と一対一に対応する情報が記憶装置内の論理ブロックに保管される。

【0032】FS管理部223は、後述するファイルシステム管理表に基づいて、LU毎のファイルシステムを指定されたNASサーバ120内のファイルシステムへ複数個をマウントすることが可能である。FS管理部223は、ファイルシステムをマウントする際に、メモリ上にマウント済みリストとして、マウントした場所、LU、ファイルシステム管理の場所を示すディスク識別子を記録する。ファイルシステム管理の場所とは、ファイルシステムのスーパーブロック、i-node、ブロック情報の保管を行うNASサーバ120内のメモリ領域である。本実施形態では、メタデータ管理部2231がこの管理を行う。なお、ファイルの情報のi-nodeやブロック情報はアクセスの高速化のために、NASサーバ内のメモリにキャッシュされてもよい。

【0033】さらに、FS管理部223は、ネットワーク処理部222から命令されるファイルオペレーションを実行する。このファイルオペレーションは、“Lookup”を行うためのファイルの検索処理、検索されたファイルの操作を一意に決定する識別子を設定するためのファイルオープン処理、識別子からファイルへの実際のアクセスを行うための読み出し処理、書き出し処理を含む。このファイルオペレーションに、i-node内の情報を変更する処理を有しても良い。FS管理部223では、このi-nodeを用いてファイルのアクセス制御を行うメタデータ管理部2231を含み、複数のPC110から同時に1つのファイルへアクセスする際にデータの一貫性保証を行っている。

【0034】ブロックデバイスプロトコル処理部224は、FS管理部223より命令された記憶領域へのオペレーションの処理をSCSIのプロトコルに従って行う。FS管理部223から命令される処理は、2つに分けられる。第1は、i-nodeの情報への読み出しと書き出し命令、第2は、ブロックの情報への読み出しと書き出し命令である。読み出し命令はSCSIプロトコルのReadに対応し、書き出し命令はWriteに対応する。本実施形態では、i-nodeの情報は、より迅速なファイルの検索と更新を実施するために、NASサーバ120内の記憶装置250に保持される。また、ブロックの情報は、i-node

ト側の記憶装置250に保持される。

【0035】記憶領域管理部225は、記憶装置となる装置を検出、管理し、デバイスブロックプロトコル処理部224で発行された命令を、命令先のLUに対して実行する。記憶装置の検出は、ローカルの記憶装置215に関しては、SCSIのLUの検出方法を用いて行われる。また、データセンタ20にある記憶装置250の検出は、NASサーバ120とデータセンタ20内のLAN240との間で通信路が確立したあと、iSCSIのプロトコルに従って、記憶装置へのIPアドレスと記憶装置上のLUへのiSCSI名を用いて行われる。検出され記憶装置は、ローカルもしくはデータセンタ毎のLUとして利用される。記憶領域管理部225は、デバイスブロックプロトコル処理部224で発行された命令に応じて、管理しているローカルもしくはデータセンタのLUを指定したSCSIの命令を実行する。

【0036】設定制御部226は、ネットワークプロトコル処理部221、ネットワークFS処理部222、FS管理部223、そして記憶領域管理部225を統合的に管理する。

【0037】設定部229は、設定制御部226に対する設定時のパラメータを入力する。

【0038】設定制御部226は、他の各部の設定に関する情報を記録するため、ディスク管理表、接続パス管理表、セキュリティ保護装置管理表、ファイルシステム管理表、エクスポート管理表、及びファイルアクセス管理表を持つ。

【0039】ディスク管理表は、ブロックプロトコル処理部224で利用され、記憶装置250から広域網30を通じて提供されるLUごとに、そのユニークな名前であるディスク識別子、LUのネットワーク上での所在を示すIPアドレス、LUへの接続後にアクセスする記憶装置のiSCSI名などの情報を保持する。

【0040】接続パス管理表は、記憶領域管理部225で利用され、記憶装置250等のIPアドレス、そして、計算機システム10からデータセンタまでの経路上に設けられるセキュリティ保護装置のIPアドレスもしくはホスト名が登録される。本実施形態では、計算機システム10のセキュリティ保護装置140からデータセンタ20へアクセスする際、セキュリティ保護装置の数は1つであるが、複数のセキュリティ保護装置が存在した場合、セキュリティ保護装置の数のIPアドレスもしくはホスト名を有する。

【0041】セキュリティ保護装置管理表は、各セキュリティ保護装置のIPアドレスまたはホスト名に対応して、そのセキュリティ保護装置での認証処理に用いられる認証情報が登録される。

【0042】ファイルシステム管理表は、FS管理部223で利用され、NASサーバ120でマウントするファイルシステムの情報に含まれる。その情報には、ロー

イルシステムを保管するＬＵのディスク識別子と、このディスク識別子で示されるＬＵのファイルシステムをマウントする場所が記述されている。例えば、ディスク識別子が“/dev/sd0a”、マウントする場所が“/mnt”だとすると、NASサーバ１２０内には“/”としてルートファイルシステムが存在するので“mnt”というディレクトリの上に“/dev/sd0a”の中に含まれるファイルシステムがマウントされる。また、ファイルシステム管理表には、NASサーバ１２０でのファイルシステムの管理方式、例えば、ファイルシステムのフォーマット、リードオンリもしくはリードとライトでファイルシステムをマウント、ファイルシステムのリカバリ方法等の情報を記述してもよい。これらについては、本実施形態の説明と直接には関係しないので説明を省略する。

【００４３】エクスポート管理表は、ネットワークＦＳ処理部２２２で利用され、複数のＰＣ１１０からのファイルオペレーションの操作をNASサーバ１２０で実施することが許可されるディレクトリを示す。これをエクスポートと呼ぶ。また、特定のＰＣ１１０に対するディレクトリ内のファイルオペレーションの許可もしくは不許可の管理を行うために、操作許可ホスト、操作不許可ホストを示す情報を含めてもよい。

【００４４】ファイルアクセス管理表は、NASサーバ１２０のメモリ上に設けられ、ファイルのアクセス状態を管理するための情報が保持される。具体的に、ファイルアクセス管理表は、メタデータ管理部２２３１において、ネットワークＦＳ処理部２２２で行われる複数のＰＣ１１０からのファイルオペレーションを管理するために使われる。

【００４５】ファイルオペレーションの管理を行うために、ファイルアクセス管理表は、各ファイルのファイル名とそのファイル識別子、及び、ファイル識別子ごとに、i-node番号、並びにファイルを参照しているＰＣ１１０を示す情報を保持したアクティブ項目を有する。また、ファイルアクセス管理表は、一度アクセスしたファイルの履歴を管理し、i-nodeのキャッシュを行うときに利用している。

【００４６】ブロックデバイスプロトコル処理部２２５は、ＳＣＳＩ等、ブロック単位で記憶装置へのアクセスが可能なプロトコルを使用する。ここでは、内部の記憶装置２１５に対してはＳＣＳＩを使用し、広域網３０経由でアクセスする記憶装置２５０に対してはＴＣＰ／ＩＰを通信路として使用するｉＳＣＳＩを使用する。

【００４７】ネットワークインタフェース２１１、２１２は、ＬＡＮあるいは広域網上に形成されるＴＣＰ／ＩＰの通信路を用い、信頼性を保証したデータの転送を行うためのインタフェースである。

【００４８】記憶装置２１５は、NASサーバでファイルシステムを構築し、ＰＣ１１０からのＬＡＮ経由での

装置２１５を磁気ディスク装置として説明するが、記憶装置として、フラッシュＲＯＭのような半導体素子を記憶媒体として用いたソリッドディスク装置や、複数のディスク装置により構成されるＲＡＩＤ装置を用いてもかまわない図４は、記憶装置２５０の構成を示す簡略化された機能ブロック図である。記憶装置２５０は、データを格納する磁気ディスク装置４２０と、磁気ディスク装置４２０へのアクセスの制御を行う記憶制御装置４１０を有する。記憶制御装置４１０は、ＬＡＮ２４０に接続するネットワークインタフェース４１５、ネットワークプロトコル処理部４１４、ブロックデバイスプロトコル処理部４１３、ファイバチャネル（ＦＣ）、ＳＣＳＩ等を介して、ディスク装置４２０に接続するチャネルインタフェース（チャネルＩ／Ｆ）４１１を有する。

【００４９】ネットワークプロトコル処理部４１４は、ＬＡＮ２４０を介して送られてくるメッセージをＬＡＮ２４０上でのＴＣＰ／ＩＰなどのプロトコルに従って処理し、アクセス要求を解釈する。また、磁気ディスク装置４２０から読み出されたデータをＬＡＮ２４０上のプロトコルに従ったメッセージとしてＬＡＮ２４０に送信する。

【００５０】ブロックデバイスプロトコル処理部４１３は、ＬＡＮ２４０を介して送られてきたアクセス要求からディスク装置４２０への操作を抽出し、チャネルインタフェース４１１を介し、磁気ディスク装置４２０のデータをアクセスする。

【００５１】記憶装置２５０は、単体の磁気ディスク装置４２０を用いた記憶装置の他、複数の磁気ディスク装置を用いたディスクアレイなどの記憶装置でもよい。記憶制御装置４１０は、１台の磁気ディスク装置４２０の記憶領域を複数の領域に分割し、分割された記憶領域をＬＵとして、あるいは、複数の磁気ディスク装置４２０に跨る記憶領域を１つのＬＵとして提供することができる。このような記憶領域の管理については、技術的に公知のものを適用することができるので、ここでは説明を省略する。

【００５２】本実施形態では、記憶媒体に磁気ディスクを適用した記憶装置を用いているが、例えば、光ディスクなど他の記憶媒体を用いた記憶装置であってもかまわない。さらに、記憶制御装置４１０は、図には示されていないが、磁気ディスク装置４２０に格納されるデータのコピーを一時的に保持するキャッシュを備えることができる。

【００５３】図５は、セキュリティ保護装置の構成を示す機能ブロック図である。ここでは、セキュリティ保護装置１３０を例に説明するが、セキュリティ保護装置２３０も同様に構成される。

【００５４】セキュリティ保護装置１３０は、プロセッサ５１０、ネットワーク（広域網３０、NASサーバ１

フェース520、及び、後述する内部認証部506、外部認証部508での認証処理に使用される認証情報を格納した認証情報データベース（認証情報DB）530を格納した記憶装置とを有する。

【0055】プロセッサ510は、TCP/IPのプロトコルに従ってメッセージ処理を行うネットワークプロトコル処理部505、内部ネットワークから広域網30を介して外部のネットワークへ接続する際に認証処理を行う内部認証部506、内部認証部506での認証の後、外部のネットワークに暗号化された通信路の設定を要求するパス接続部507、外部から内部ネットワークへの接続に対する認証処理を行う外部認証部509、外部処理認証部509で認証された通信に対して暗号化された通信を確立するパス確立部508、及び、ネットワーク経由で認証情報の登録、管理を行う認証情報管理部501を有する。これら各部の機能は、プロセッサ510上でのプログラム処理により実現される。

【0056】認証情報DB502には、認証情報として、接続相手側のセキュリティ保護装置と暗号化を行うための暗号鍵、暗号鍵の寿命、認証アルゴリズム、暗号アルゴリズム、及び相手側セキュリティ保護装置のIPアドレスもしくはホスト名等の情報が格納されている。

【0057】セキュリティ保護装置130は、他に、図示されていないプロセッサ510により実行されるプログラムを格納するためのメモリや、通信されるメッセージをキャッシングするためのキャッシュメモリ等を有する。

【0058】図6は、NASサーバ120の設定処理を示すフローチャートである。この処理は、PC110からNASサーバ120の利用に先立って、あるいは、必要に応じて適宜実施される。

【0059】NASサーバ120の設定では、まず、LUの設定が行われる（ステップ600）。

【0060】続いて、利用可能なファイルシステムの存在が判別される。NASサーバ120は、LUに保持されている利用可能なファイルシステムの有無を、LU内の1ブロックに記述されているスーパーブロックのマジックナンバを参照して判定する。利用可能なファイルシステムが存在しない場合には、ステップ604において、ファイルシステムが構築される（ステップ602）。

【0061】ファイルシステムが存在すれば（あるいは、構築された後）、そのファイルシステムが当該NASサーバ120にマウントされているか判別する。この判別は、FS管理部223により記録されたマウント済みリストを参照して行われる。ファイルシステムが、マウントされていない場合は、ステップ608において、ファイルシステムのマウント処理が実施される（ステップ606）。

がエクスポート済みか否か判別される。この判別は、ネットワークFS処理部222のエクスポート管理表に保持された情報の有無に基づいて行われる。ファイルシステムがエクスポートされていない場合は、ステップ612でファイルシステムのエクスポートが実施される（ステップ610）。

【0063】図7は、ステップ600において実施されるLUの設定処理の流れを示すフローチャートである。この処理により、ローカル及びリモートに存在するLUがNASサーバ120により認識される。

【0064】NASサーバ120は、管理者より、割り当てるLUの存在場所が、NASサーバ120内のLUであるか、データセンタ20内のLUであるかの選択を受け付ける（ステップ700）。

【0065】管理者によりNASサーバ120内のLUが選択された場合、NASサーバ120は、記憶装置215の全LUNにSCSIのInquiryコマンドを発行してLUを検出し、そのLUを識別可能な情報を表示装置（図示せず）に表示する（ステップ702）。

【0066】続いて、NASサーバ120は、ブロックデバイスプロトコル処理部224により計算機システム10とデータセンタ20内で一意に決定されるディスク識別子を登録して、LUの設定処理を終了する（ステップ704）。

【0067】ステップ700において選択されたLUが、データセンタ20内に存在する場合、NASサーバ120は、管理者より、リモートサイトにあるLUの位置情報を受け付ける。LUの位置情報としては、記憶装置250のIPアドレスまたはホスト名、iSCSIで用いられLUを一意に決定するiSCSI名が用いられる。

ここで、ディスク識別子とiSCSI名は、共に基本的にはLUを示すが、ディスク識別子にはデバイスへの接続経路となるI/F212の情報が含まれる。このため、ディスク識別子は、複数のI/Fが存在したとしても、一意なLUを決定することができる（ステップ708）。

【0068】続いて、入力された位置情報を用い、記憶装置250のLUへの接続が試みられ、接続の可否が判別される（ステップ710）。接続に成功した場合、ステップ704の処理に移る。一方、接続に失敗した場合、ステップ712において、記憶装置250のLUへの通信路を確立させた後、ステップ704の処理に移る（ステップ712）。

【0069】図8は、ステップ712において実施される、外部にある記憶装置250への通信路の確立処理を示すフローチャートである。この処理により、記憶装置250への通信路の確保がされる。

【0070】まず、NASサーバ120は、管理者より、データセンタ20のセキュリティ保護装置230に関する認証情報の入力を受け取る。そして、入力された情報に基づき、先に述べたように、記憶装置250の通信路を確立する。

作成される（ステップ800）。

【0071】続いて、NASサーバ120は、接続パス管理表の該当するパスのエントリに登録された情報に基づいてセキュリティ保護装置の数を取得し、セキュリティ保護装置の段数を変数“S”に設定する（ステップ802）。

【0072】NASサーバ120は、セキュリティ保護装置130へ接続する。このとき、セキュリティ保護装置130の安全性を高めるために認証して接続を行ってもよい（ステップ804）。

【0073】NASサーバ120は、データセンタ20に到達する経路に存在する複数のセキュリティ保護装置230の一つに広域網経由でTCP/IPを用いて接続する（ステップ806）。この後、セキュリティ保護装置130にデータセンタ側のセキュリティ保護装置230との接続に必要な認証情報として、セキュリティ保護装置管理表に登録されている認証情報が渡される。NASサーバ120は、この認証情報による認証の可否を判定する（ステップ807）。

【0074】ステップ807において、認証に成功すると、NASサーバ120は、変数Sの値を1減算する（ステップ808）。そして、Sが0になったか否か、すなわち、すべてのセキュリティ保護装置について認証が完了したか判別する（ステップ810）。すべてのセキュリティ保護装置について認証が完了すると、NASサーバ120は、セキュリティ保護装置130と230との間で通信路を確立し、目的のLUが含まれる記憶装置250への接続を行う（ステップ812）。

【0075】ステップ810において、S>0、すなわち認証が完了していないセキュリティ保護装置がある場合、処理はステップ806に戻り、次のセキュリティ保護装置への認証が行われる。

【0076】ステップ807において、セキュリティ保護装置の認証に失敗した場合、NASサーバ120は、認証の済んだ全てのセキュリティ保護装置との間の論理的な通信路を切断し、設定処理を終了する（ステップ814）。

【0077】図9は、ステップ608で実施されるファイルシステムの構築処理の流れを示すフローチャートである。この処理により、認識されたLU上の記憶領域に、ファイルシステムが存在していない場合、あるいはファイルシステムを作成する場合に、ファイルシステムが構築される。

【0078】ファイルシステムの構築処理では、NASサーバ120は、FS管理部223によりLU設定処理（ステップ604）で検出されたLUを示すディスク識別子を選択する。このとき、各記憶領域上のファイルシステムの存在が、前述のスーパーブロックを確認することにより調べられる。ファイルシステムが存在すると、

構築されているLUに対応して表示される（ステップ900）。

【0079】続いて、NASサーバ120は、ステップ900でディスク識別子が表示された画面上で、管理者より、ファイルシステムを構築するLUに対応したディスク識別子の選択を受け付ける（ステップ902）。

【0080】次に、NASサーバ120は、選択されたLUに対するフォーマットを行うか否かを管理者に問い合わせる（ステップ904）。管理者によりフォーマットが指示されなければ、ファイルシステムの構築処理は終了する。管理者により、フォーマットが指示された場合は、選択された記憶領域のフォーマットを実施する。このフォーマットにより、前述のファイルシステムを構成する要素であるスーパーブロック、i-node、そして、ブロックが、選択されたLUに形成される（ステップ906）。

【0081】図10は、ステップ612で実施されるファイルシステムのマウント処理のフローチャートである。

【0082】マウント処理では、まず、管理者よりマウントするディスク装置250内LUの識別子が登録される。このとき、表示装置には、例えば、NASサーバ120から認識できるLUのディスク識別子、そのLUに構築されているファイルシステムの名称（ある場合）、及びLUのマウントポイント名（LUがマウント済みの場合）が対応づけられて表示される。管理者は、表示されたディスク識別子の中から、マウントしようとするLUのディスク識別子を選択する（ステップ1000）。

【0083】続いて、NASサーバ120は、選択されたLU内のファイルシステムがマウント可能であるか否かを、FS部223がメモリ内に管理しているファイルシステムのマウント済みリストから判別する（ステップ1002）。

【0084】選択されたLUのファイルシステムがマウント可能な場合、管理者からマウントポイントの指定を受け付ける（ステップ1004）。マウントポイントが指定されると、ステップ1000で選択されたLU内のファイルシステムが、指定されたマウントポイントでNASサーバ120にマウントされる（ステップ1006）。NASサーバ120は、LUのファイルシステムをマウント時、ファイルシステムを利用可能にする初期状態を作るために、ファイルシステムのスーパーブロック内の情報から1番目のi-node情報（ファイルシステムの基底となるルートディレクトリ）を読み出し、メモリ内に登録して処理を終了する（ステップ1008）。

【0085】一方、ステップ1002において、ファイルシステムのマウントができないと判断されると、エラーが管理者に通知され、NASサーバの設定処理が終了する（ステップ1010）。

【0086】図11は、ステップ612で実施されるファイルシステムのマウント処理のフローチャートである。

が、NASサーバ120は、マウント済みのファイルシステムの管理を終了する際には、そのファイルシステムをアンマウントする。アンマウントでは、まず、FS部のメモリ上で管理が行われているファイルシステムのi-node情報、ブロック情報、スーパーブロックの更新分がメモリからLUへ書き出され、FS管理部223内のマウント済みリストから該当ファイルシステムのエントリが削除される。

【0087】続いて、本実施形態におけるファイルのアクセス処理について説明する。

【0088】各PC110は、ファイルをアクセスしようとするとき、NASサーバ120によって公開されているLUを、LAN140を介してマウントする。PC110は、NOS112により提供されるファイルオペレーションを用いて、マウントされたボリューム内のファイルをアクセスする。ファイルオペレーションの代表的なものには、オープン、リード、ライト、クローズなどがある。

【0089】特定のファイルをアクセスする際には、ファイルハンドラと呼ばれるファイルごとに一意に決定される識別子が用いられる。このファイルハンドラは、ファイルのオープン時に取得される。

【0090】図12は、NASサーバ120で実施されるファイルアクセス処理の概略を示すフローチャートである。この処理は、PC110からファイルオペレーションを用いて発行された、ファイルのオープン、クローズ、リード、ライトなどの要求に応じて実施される。

【0091】PC110からのファイルのアクセス要求が発生すると、ネットワークFS管理部222は、FS管理部223のファイルオペレーションを利用してメタデータ管理部2231に対して、要求された種別のファイルオペレーションに関するアクセスの許可を求める（ステップ1202）。

【0092】メタデータ管理部2231からファイルへのアクセス制御に関する応答があると、ネットワークFS管理部222は、その応答に基づいてアクセスの可否を判別する（ステップ1206）。

【0093】アクセスが許可された場合、FS管理部223は、ブロックデバイスプロトコル処理部224に指示し、SCSI等のブロックデバイスプロトコルを用いたLUへのブロック単位でのリードとライト処理を行う。記憶領域管理部225は、対象とされるLUが記憶装置215にあるとき、記憶装置215内のLUに対してアクセス処理を実施する。また、対象とされるLUがデータセンタ20にあるとき、記憶領域管理部225は、データセンタ20の該当する記憶装置250のLUにアクセスする（ステップ1208）。

【0094】ステップ1206において、アクセスが許可されていない場合、ネットワークFS管理部222は、エラーを通知して処理を終了する（ステップ1209）。

10）。

【0095】図13は、ファイルのオープン処理におけるステップ1202の処理を示すフローチャートである。

【0096】NASサーバ120がPC110から特定のファイルに対するオープン要求を受け付けると、その要求は、ネットワークFS処理部222に入力される。ネットワークFS処理部222は、FS管理部223に、PC110からのオープン要求で指定されたファイルのオープンを求める。FS管理部223は、その要求をメタデータ管理部2231に渡す（ステップ1300）。

【0097】メタデータ管理部2231は、ファイルアクセス管理表を参照して、指定されたファイルがすでにオープンされているか判別する。具体的には、ファイルアクセス管理表の当該ファイルに関するアクティブ項目に、いずれかのPCにより参照されていることを示すホスト名もしくはIPアドレスとファイル識別子の情報がセットされているか否かが調べられる（ステップ1302）。

【0098】メタデータ管理部2231は、指定されたファイルがオープンされていない場合は、ファイルアクセス管理表に当該ファイルのエントリを作成し、i-node情報とディスク識別子を設定する。また、アクティブ項目に、オープン要求を発行したPC110のホスト名を設定する（ステップ1304）。

【0099】次に、メタデータ管理部2231は、ファイルアクセスに用いられるユニークな識別子を要求元のネットワークFS処理部222に戻す（ステップ1306）。

【0100】一方、ステップ1302において、ファイルが既にオープンされていると判定されたとき、メタデータ管理部2231は、ファイルアクセス管理表の該当ファイルのレコードにPC110のホスト名とファイルの識別子を追加する（ステップ1308）。そして、ステップ1306においてファイル識別子に戻し、このファイル識別子を用いたアクセスを可能にする。

【0101】図14は、ファイルのリード処理におけるステップ1202の処理を示すフローチャートである。

【0102】NASサーバ120がPC110から特定のファイルデータのリード要求を受け付けると、その要求は、ネットワークFS処理部222に入力される。ネットワークFS処理部222は、FS管理部223に、その要求を送る（ステップ1400）。

【0103】FS管理部223は、その要求をメタデータ管理部2231に渡す。メタデータ管理部2231は、ステップ1302と同様にして、リードの対象となるファイルがオープンされていてアクティブな状態か否かを調べる（ステップ1402）。

【0104】ファイルがすでにオープンされている場合、メタデータ管理部2231は、ファイルアクセス管理表の当該ファイルのレコードに、リード要求を発行したPC110のホスト名とファイル識別子を追加する（ステップ1404）。

に、メタデータ管理部2231は、ファイルアクセス管理表を参照して、ファイルを共有している他のPC110が存在するか調べる（ステップ1404）。ファイルを共有しているPC110がある場合、メタデータ管理部2231は、そのPC110に対して、バッファリングしているデータの記憶装置250への書き戻しを指示し、ファイルデータの一貫性を保証する（ステップ1406）。

【0105】ステップ1402において、ファイルがオープンされていなかったとき、ステップ1404において、ファイルが他のNASサーバにより共有されていなかったとき、あるいは、ステップ1406の処理により、記憶装置にデータが書き戻された後、ファイルアクセス管理表のi-node情報から、読み出すデータの範囲を示すブロック位置情報を取得し、ネットワークFS処理部222に返す（ステップ1408）。

【0106】以上の処理の後、NASサーバ120は、ステップ1208の処理により、受け取ったブロック位置情報に基づいて、記憶装置からデータを読み出す。読み出されたデータとそのサイズは、記憶領域管理部225からネットワークFS処理部222に返される。PC110は要求したリード処理の戻り値としてサイズとデータが含まれるメモリ領域を取得する。

【0107】図15は、ファイルのライト処理におけるステップ1202の処理を示すフローチャートである。

【0108】NASサーバ120がPC110からファイルへのライト要求を受け付けると、その要求は、ネットワークFS処理部222に入力される。ネットワークFS処理部222は、FS管理部223にその要求を送る（ステップ1500）。

【0109】続いて、ステップ1402～1406と同様に、ファイルが既にアクティブか（ステップ1502）、ファイルを共有するPC110があるか調べられ（ステップ1504）、ファイルを共有するPC110がある場合に、バッファリングしているデータの書き出しの指示が行われる（ステップ1506）。

【0110】以上の処理の後、メタデータ管理部2231は、データを書き込むための領域（ブロック）が記憶装置215、250に確保できるか調べ、確保できれば、データ書き込みのためにその領域を割り当てる。ここでのブロックの割り当ては、従来の一般的なファイルシステムにより行われるブロックの割り当てと同様にし行われる（ステップ1508）。

【0111】領域の割り当てがすむと、割り当てられた領域の位置情報としてそのブロックアドレスがメタデータ管理部2231からFS管理部223に返される（ステップ1510）。

【0112】NASサーバ120は、この後、FS管理部223に返されたブロックアドレスに基づいて、記憶

む。データの書き込みが終了すると、書き込まれたデータのサイズが、FS管理部223からネットワークFS処理部222に返され、要求元のPC110に、戻り値としてネットワークFS処理部222から書き込まれたデータサイズが送られる。

【0113】ステップ1508で領域の確保ができなかった場合は、ライトアクセス不可として、エラーが返され、要求元のPC110にその旨が通知される（ステップ1512）。

【0114】図16は、ファイルのクローズ処理におけるステップ1202の処理を示すフローチャートである。

【0115】クローズ処理では、オープン処理と同様に、要求がネットワークFS処理部222で受け付けられ（ステップ1600）、対象とされるファイルがオープンされているか調べられる（ステップ1602）。

【0116】ファイルがオープンされていれば、該当するファイルについての情報をファイルアクセス管理表から削除する（ステップ1604）。ファイルアクセス管理表から該当ファイルのエントリを削除した後、ファイルのクローズに成功したことを通知して処理を終了する（ステップ1606）。

【0117】一方、ステップ1602で該当するファイルがオープンされていないと判断されたときは、メタデータ管理部はエラーを通知して処理を終える（ステップ1608）。

【0118】図18は、セキュリティ保護装置130、230間の認証動作の手順を示すフローチャートである。

【0119】まず、NASサーバ120からセキュリティ保護装置130へTCP/IPで接続し（ステップ1800）、前述の認証情報を設定する（ステップ1801）。この時の、TCP/IPでの接続において、内部からもセキュリティの維持をするために内部認証部506でNASサーバ120からの認証を行ってもよい。外部にあるセキュリティ保護装置へは、認証情報に記述されているそのセキュリティ保護装置のIPアドレスを用いてTCP/IPを用いて接続する（ステップ1802）。

【0120】続いて、接続相手側のセキュリティ保護装置230に認証情報を送付する。相手側セキュリティ保護装置では、外部認証部509により送付された認証情報と、認証情報DB530に保持されている認証情報と比較して認証する（ステップ1806）。

【0121】認証に成功すれば、パス接続部507において、外部のセキュリティ保護装置との間で、認証情報内の暗号化アルゴリズムを元に暗号化された通信路による接続を行う（ステップ1808）。

【0122】ステップ1806で認証に失敗した場合は、接続元装置との間の接続が断たれる（ステップ1810）。

【0123】以上のような処理により、NASサーバ120から自システム内のセキュリティ保護装置130、データセンタ20のセキュリティ保護装置230、そして記憶装置250それぞれの間に論理的な通信路を張ることができる。また、自システム内と他システム内でIPアドレスの管理形態が異なる場合があるが、このような場合は、自システムと他システム内のIPアドレスを変換する機構、例えば、Network Address Translator (NAT) の機能をセキュリティ保護装置内に組み込んでもよい。

【0124】以上説明した実施形態によれば、PCからLAN経由でNASサーバにより提供される記憶装置を利用できる。NASサーバは、自サーバ内、あるいは外部に持つことが可能で、PCに対して、記憶装置の物理的な場所を隠蔽することができる。PCのユーザは、NASサーバにより提供される記憶領域を利用するに際し、データの記憶位置を意識することなく記憶装置を利用することができる。

【0125】上述した実施の形態では、データセンタにある記憶装置を、異なる計算機システム10に存在する複数のNASサーバから共有した場合に、記憶装置に保持されたデータの一貫性を維持できなくなる恐れがある。以下に、複数のNASサーバから一貫性を維持した記憶装置の共有に配慮した計算機システムの一例について説明する。

【0126】図19は、本発明の第2の実施形態における計算機システムの簡略なブロック図である。

【0127】本実施形態における計算機システムは、複数の計算機システム10がデータセンタ50と広域網30を介して接続される。本実施形態では、各計算機センタ10のNASサーバ120において行われる処理が一部変更される点、及び、データセンタ50にNASサーバ管理ホスト210が設けられる点を除き、第1の実施形態とほぼ同様の構成を有する。

【0128】NASサーバ管理ホスト210は、NASサーバ120間でファイルを共有する際に必要な排他管理、アクセス管理等を行う。なお、ここでは、NASサーバ管理ホスト210が1台の場合について説明するが、複数台のNASサーバ管理ホスト210を設け、記憶装置250により提供される記憶領域のファイルシステムを、これら複数のNASサーバ管理ホスト210で分散して管理してもよい。

【0129】図3は、NASサーバ管理ホスト210の構成を示す機能ブロック図である。NASサーバ管理ホスト210は、複数のNASサーバ120で共用されるデータセンタ20内の記憶装置250に記録されたファイルに対するデータの保証を行うための共有時のアクセス制御を行う。本実施形態では、アクセス制御をNASサーバ管理ホスト210で行うが、NASサーバ管理ホ

関する制御を備えていてもよい。

【0130】NASサーバ管理ホスト210は、ネットワークインタフェース310、330とプロセッサ320を有する。この他、NASサーバ管理ホスト210は、メモリや入出力装置などを有するが、これらは、本発明の説明と直接関係するものではなく、図示を省略する。

【0131】プロセッサ320は、ネットワークインタフェース310を介して受信したNASサーバ120からのファイルへのアクセスを制御する。このためにプロセッサ320は、ネットワークプロトコル処理部321、ファイルシステム管理部(FS管理部)322、ブロックデバイスプロトコル処理部323、制御部324を有する。プロセッサ320の有する各部の機能は、プロセッサ320上でのプログラム処理により実現される。

【0132】ネットワークプロトコル処理部321は、ネットワークプロトコル処理部221と同様に、TCP/IPのプロトコルに従ってNASサーバ120からのアクセス要求の受信処理、及び、NASサーバ120へのファイルデータの送信処理を行う。ネットワークプロトコル処理部321は、NASサーバ120からのアクセス要求の受信処理では、受信した要求をFS管理部322に渡す。

【0133】FS管理部322は、NASサーバ120のFS管理部223と同様、LU上のファイルシステム情報を読み取り、初期状態をつくるマウント処理と終了時のアンマウントの処理、FS部223より要求されたファイルのアクセス要求をメタデータ処理部へ転送する機能を持つ。

【0134】メタデータ管理部3221では、アクセス中のファイルに関するi-node情報を含むファイルアクセス管理表を用いてファイルのアクセス管理を行い、複数のNASサーバ120によりファイルが共有された時には、FS管理部223より転送されたアクセス要求に対するデータのー貫性を保証する。特に、ファイルのデータやi-node情報がNASサーバ120のFS管理部223でバッファリングされているときには、そのデータを一度フラッシュした後で、ファイルへのアクセスを行うよう制御する。また、第1の実施形態におけるファイルシステム管理表に記載されているマウントするファイルシステムの情報にファイル共有を許可するNASサーバ120のホスト名もしくはIPアドレスを加える。このホスト名もしくはIPアドレスは1つもしくは複数個あってもよい。

【0135】複数のNASサーバ120間で記憶装置250内のLU内のファイルシステムが共有される場合、NASサーバ管理ホスト210のメタデータ管理部3221でファイルアクセス管理表が管理される。このた

管理部223は、マウント済みリストの項目として、第1の実施形態において説明した情報の他、他のNASサーバとの間でLUの共有が生じている場合に、その共有を管理するNASサーバ管理ホスト210のホスト名、あるいは、IPアドレスを保持する。また、NASサーバ120のメタデータ管理部2231で利用されるファイルアクセス管理表は、メタデータ管理部3221においても保持、管理される。

【0136】制御部324は、NASサーバ120から要求命令されるNASサーバ管理ホスト210の設定を行う。

【0137】本実施形態では、他のハードウェア構成については、第1の実施形態と同じであり、説明を省略する。

【0138】本実施形態におけるNASサーバの設定は、図6に示した第1の実施形態におけるものとほぼ同様に行われる。ただし、本実施形態では、LUの共有が発生するため、ステップ614（または616）の処理の後に、NASサーバ間でのLU内ファイルシステムの共有の設定が行われる。

【0139】具体的には、データセンタ20にあるLU上のファイルシステムの共有の有無が管理者により選択される。データセンタ20のLU上のファイルシステムを共有しない場合は、設定処理は終了する。NASサーバ120間でファイルシステムを共有する場合は、NASサーバ120間でのファイルシステムの共有設定を行った後、設定を終了する。

【0140】図11は、NASサーバ間でLU内のファイルシステムの共有を設定するための手順を示すフローチャートである。この処理により、複数のNASサーバ120間で共有されるLUの管理が、NASサーバ管理ホスト210に移管される。

【0141】管理者は、複数のNASサーバで共有しようとするファイルシステムを格納したLUを管理しているNASサーバ120に対して、共有しようとするファイルシステムの移管に関する情報を入力する。移管に関する情報には、共有されるLUとファイルシステムの指定が含まれる。（ステップ1100）。

【0142】ステップ1100で指定されたLUが、NASサーバ120内の記憶装置215の記憶領域内にある場合、データセンタ20にある記憶装置250に選択されたLUの複製が作成される。LUの複製作成には、いわゆるリモートコピーと呼ばれる技術を利用できる。なお、選択されたLUが記憶装置250内に形成されたLUであるときは、この処理は省略される（ステップ1102）。

【0143】次に、NASサーバ120内のFS管理部223、メタデータ管理部2231の動作を一時的に停止（凍結）させる（ステップ1104）。さらに、NAS

サーバ120は、変更されているファイルに関するinode情報（ファイル管理情報）を含むメタデータをLU内の所定の領域に吐き出す。メタデータの吐き出し処理が終了した後、NASサーバ120は、ステップ1102で行ったLUの二重化を停止する（ステップ1106）。

【0144】NASサーバ120は、ファイルの管理を移管するNASサーバ管理ホスト210との間の通信路を確立させる。通信路を確立するための処理は、図8において説明した、NASサーバ120と記憶装置250との間の通信路の確立処理と同様にして行われる（ステップ1108）。NASサーバ管理ホスト210との間の通信路を確保すると、NASサーバ120は、ファイルアクセス管理表の情報の内、他のNASサーバ120と共有するファイルに関する情報をNASサーバ管理ホスト210に送る（ステップ1110）。

【0145】NASサーバ管理ホスト210は、受け取ったファイルアクセス管理表の情報を参照し、アクティブとなっていたファイルをオープンする（ステップ1112）。続いて、FS管理部322を起動し、ファイルシステムの運用を開始する（ステップ1114）。

【0146】NASサーバ120では、メタデータ管理部2231が、共有ファイルに関するメタデータをNASサーバ管理ホスト210に移動し、管理を移管したことをFS管理部223に通知する（ステップ1116）。FS管理部223は、メタデータ管理部2231からの通知を受けると、処理を活性化させる（ステップ1118）。

【0147】処理が活性化された後、PC110のファイルオペレーションによりファイル操作がなされると、FS管理部223は、ファイルの操作に関してNASサーバ管理ホスト210のメタデータ管理部3221に命令を送信し、ブロックデバイスプロトコルを用いて記憶装置250と通信し、ファイルのデータを転送する。このようにして以後、NASサーバ120間でファイルの共有が可能となる。

【0148】図17は、NASサーバ管理ホスト210で管理されているファイルシステムを含むLUを新たなNASサーバから利用可能とするときに実施される処理のフローチャートである。

【0149】まず、新たに接続しようとするNASサーバ120とNASサーバ管理ホスト210との間で認証された通信路が確保される。この処理は、図8により説明した処理と同様にして行われる（ステップ1700）。

【0150】通信路が確保できた後、NASサーバ120は、接続しようとするファイルシステムを含むLUのマウントをNASサーバ管理ホスト210に要求する（ステップ1702）。

【0151】NASサーバ管理ホスト210は、新たな

NASサーバ120からマウントの要求を受けると、そのNASサーバ120が、マウントを要求されたLUのファイルに対する操作を許可されたサーバかどうか調べる。具体的には、ファイルシステム管理表のディスク識別子に対応して、共有可能なNASサーバとしてホスト名若しくはIPアドレスが登録されているか調べる。ファイルシステム管理表にホスト名が設定されていれば後続のファイルの操作が許され、ホスト名若しくはIPアドレスが設定されていなければ、公開は許可されない。後者の場合、ステップ1706でエラーがNASサーバ120に返され処理が終了する(ステップ1704)。

【0152】公開が許される場合、NASサーバ管理ホスト210は、NASサーバ120に接続許可の応答を返す(ステップ1706)。

【0153】NASサーバ120は、接続が許可されると、ステップ1700と同様に、今度は、接続しようとするLUを有する記憶装置250との間で認証された通信路を確立させる(ステップ1710)。

【0154】最後に、NASサーバ120は、ファイルアクセス制御をNASサーバ管理ホスト210のメタデータ管理部3221に依頼し、後続のファイル操作を可能とする(ステップ1714)。

【0155】以上の処理により、新たなNASサーバからデータセンタに存在するファイルシステムを利用することが可能となる。NASサーバ120によって共有されているファイルシステムの利用を停止する際は、NASサーバ120で使用中のファイルへのオペレーションが完了し、バッファリングしているデータがファイルシステムを含むLUへ保管された後、ファイルシステム管理表から該当ファイルシステムのエントリが削除される。そして、第1の実施形態で説明したアンマウント処理と同様の処理がNASサーバ管理ホスト210で行われる。

【0156】PC110からファイルオペレーションを実行する際に実施される処理について、以下に説明を行う。なお、本実施形態では、NASサーバ間でLUを共有可能とするために、第1の実施形態における処理と一部異なった処理が実施される。以下、第1の実施形態におけるファイルオペレーションとの相違点を主として説明を行う。

【0157】本実施形態におけるファイルのアクセス処理では、ファイルシステムのi-node、スーパーブロック、ブロックの管理などのファイルシステム管理情報が何処で管理されているかによって処理が異なる。このため、図12におけるステップ1202の処理が、以下のようになる。すなわち、NASサーバ120は、PC110からアクセス要求を受けると、マウント済みリスト内に登録されたファイルシステム管理場所を参照し、アクセスの対象とされるLUが、NASサーバ120内のメタデータ管理部3221に、NASサーバ管理ホスト210

210内のメタデータ管理部3221のいずれで管理されているか判別する。この判別処理は、FS管理部223において行われる。アクセス対象のLUがNASサーバ120内のメタデータ管理部2231で管理されている場合は、先に説明した第1の実施形態と同様に処理が進められる。

【0158】ファイルアクセスの対象となるLUがNASサーバ管理ホスト210のメタデータ管理部3221で管理されている場合、FS管理部223は、NASサーバ管理ホスト210のメタデータ管理部3221に対してアクセス要求を送り、ファイルへのアクセス許可を求める。

【0159】NASサーバ管理ホスト210のメタデータ管理部3221は、NASサーバ120のFS管理部322からアクセス要求を受けると、ファイルのオープン、リード、ライト、及びクローズの各処理においてそれぞれ図13～図16において説明したNASサーバ120のメタデータ管理部2231と基本的に同様の処理を実施する。ただし、図13～図16の処理においても、複数のNASサーバによるLUの共有を行うために、一部の処理が異なっている。

【0160】具体的に、ファイルのオープン処理では、図13のステップ1300において、NASサーバ管理ホスト210側では、NASサーバ120からオープン要求を受け取ると、要求元のNASサーバに対して、該当するファイルシステムのアクセスが許可されているか判定する。この判定は、ファイルシステム管理表を参照し、アクセスを許可されたNASサーバとして、要求元NASサーバ120のホスト名、あるいはIPアドレスが登録されているかどうかに基づいて行われる。要求元のNASサーバ120によるファイルシステムのアクセスが許可されている場合は、以降のオープン処理を継続し、そうでなければ、エラーとして処理を中断する。

【0161】ファイルデータのリード処理時、図14におけるステップ1404でメタデータ管理部3221は、他のNASサーバ120との間でファイルの共有がされているかファイルアクセス管理表を参照して判別する。ファイルの共有がある場合は、第1の実施形態において説明した処理の他、ステップ1406で他のNASサーバに対し、バッファリング中のデータの書き出しを要求し、データの一貫性を保証する。

【0162】ファイルデータのリード処理時、メタデータ管理部3221は、図15のステップ1504において、上述したファイルデータのリード時と同様に、他のNASサーバ120との間でファイルの共有がされているか判別する。ファイルを共有しているNASサーバがあれば、メタデータ管理部3221はステップ1506で他のNASサーバにバッファリングしているデータの書き出しを要求する。

【0163】ファイルのクローズ時、他のNASサーバ

との間でファイルが共有されているときは、ステップ1604においてメタデータ管理部3221は、該当するレコードを削除することに代えて、クローズ要求元のNASサーバに関連する情報を当該レコードから削除し、レコード自体は残す。該当レコードは、ファイルを利用するNASサーバがなくなった時点で削除される。

【0164】なお、本実施形態では、NASサーバ管理ホストは、データセンタに設置され、NASサーバとは広域網を介して接続されるが、例えば、企業内計算機システムのいずれかにNASサーバ管理ホストを設置することも可能である。この場合、その企業内計算機システムのNASサーバとNASサーバ管理ホストとは、LANを介して接続される。

【0165】以上説明した実施形態によれば、異なる計算機システム上のPCのユーザが、NASサーバから適用される広域網上の記憶装置上のファイルシステムを通じて、単一ファイルを共有することが可能となる。

【0166】

【発明の効果】本発明によれば、記憶装置の利用者がデータの保管場所を意識することなく、広域網やLANを介して安全にデータを保管し、あるいはデータの共有をすることができる。

【図面の簡単な説明】

【図1】発明が適用された計算機システムの一実施形態における構成を示す簡略なブロック図である。

【図2】NASサーバの構成を示す機能ブロック図である。

【図3】NASサーバ管理ホストの構成を示す機能ブロック図である。

【図4】記憶装置250の構成を示す簡略化された機能ブロック図である。

【図5】セキュリティ保護装置の構成を示す機能ブロック図である。

【図6】NASサーバの設定処理の流れを示すフローチャートである。

【図7】LU設定処理の流れを示すフローチャートである。

【図8】外部の記憶装置への通信路の確立処理を示すフローチャートである。

【図9】ファイルシステムの構築処理の流れを示すフローチャートである。

【図10】ファイルシステムのマウント処理のフローチャートである。

【図11】NASサーバ間でのLUの共有処理のフローチャートである。

【図12】NASサーバで実施されるファイルアクセス処理の概略を示すフローチャートである。

【図13】ファイルのオープン処理におけるステップ1202の処理を示すフローチャートである。

【図14】ファイルのリード処理におけるステップ1202の処理を示すフローチャートである。

【図15】ファイルのライト処理におけるステップ1202の処理を示すフローチャートである。

【図16】ファイルのクローズ処理におけるステップ1202の処理を示すフローチャートである。

【図17】NASサーバ管理ホストで管理されているファイルを新たなNASサーバから利用可能とするときに実施される処理のフローチャートである。

【図18】セキュリティ保護装置の認証動作の手順を示すフローチャートである。

【図19】発明が適用された計算機システムの第2の実施形態における構成を示す簡略なブロック図である。

【符号の説明】

110・・・パーソナルコンピュータ

120・・・NASサーバ

130、230・・・セキュリティ保護装置

210・・・NASサーバ管理ホスト

250・・・記憶装置

221、321、414・・・ネットワークプロトコル処理部

222・・・ネットワークファイルシステム処理部

223、322・・・ファイルシステム管理部

224、323、413・・・ブロックデバイスプロトコル処理部

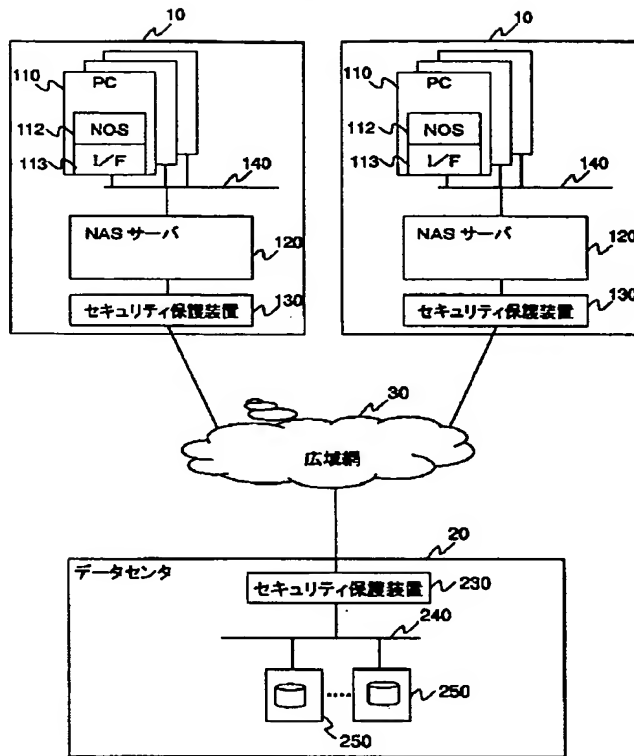
225・・・記憶領域管理部

227・・・セキュリティ処理部

228・・・設定制御部

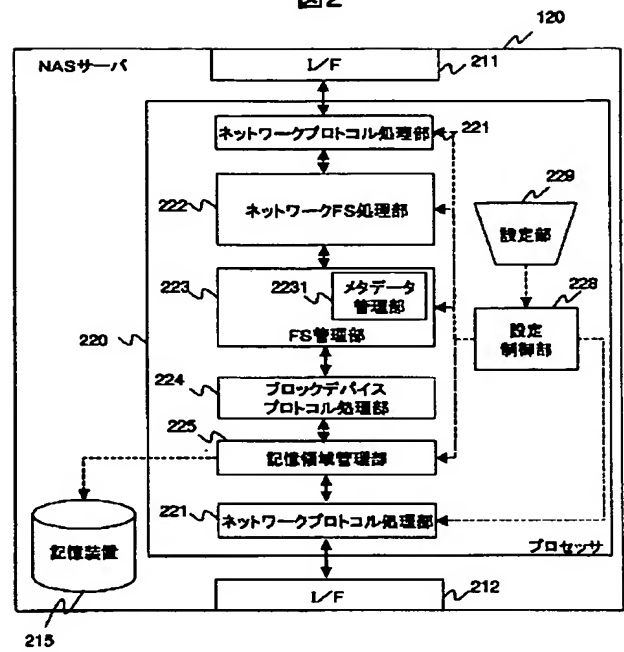
【図1】

図1



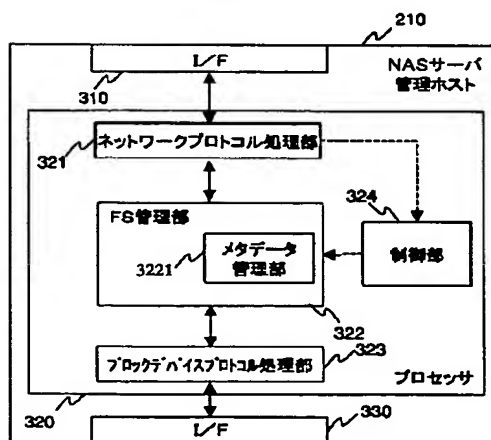
【図2】

図2



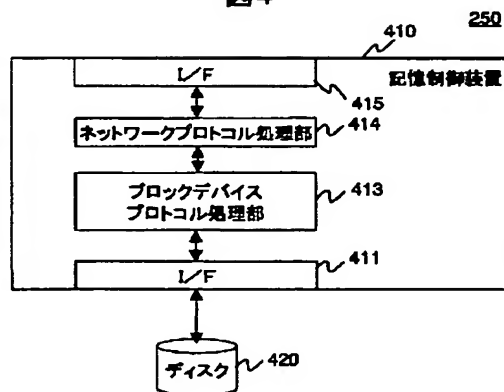
【図3】

図3



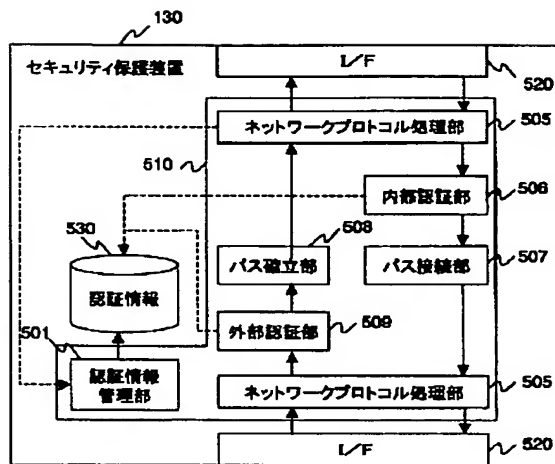
【図4】

図4



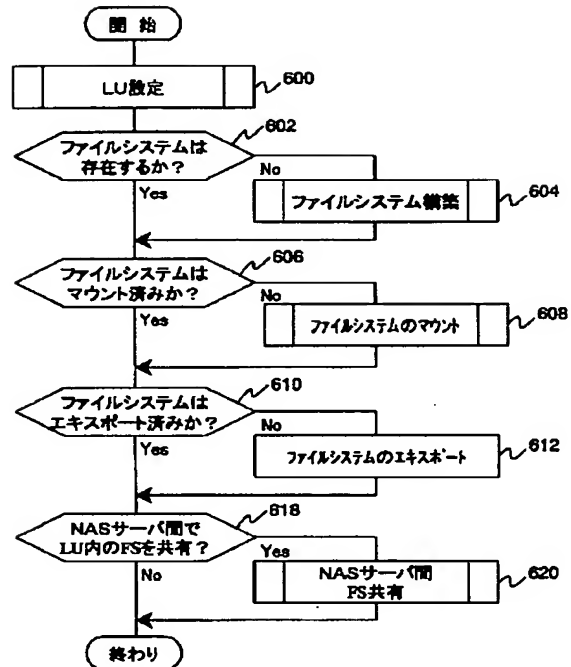
【図5】

図5



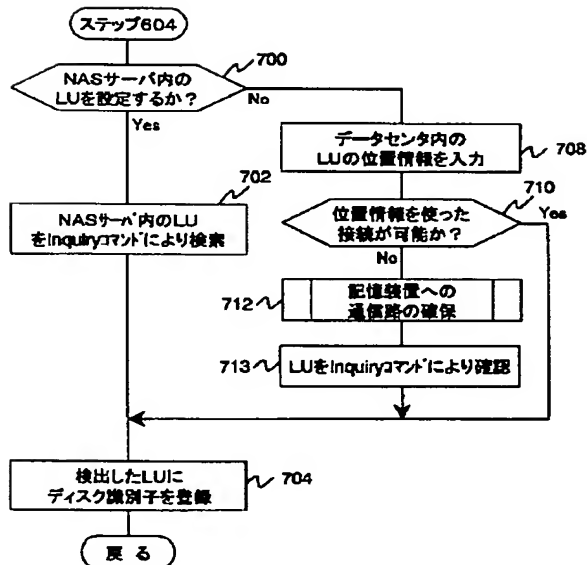
【図6】

図6



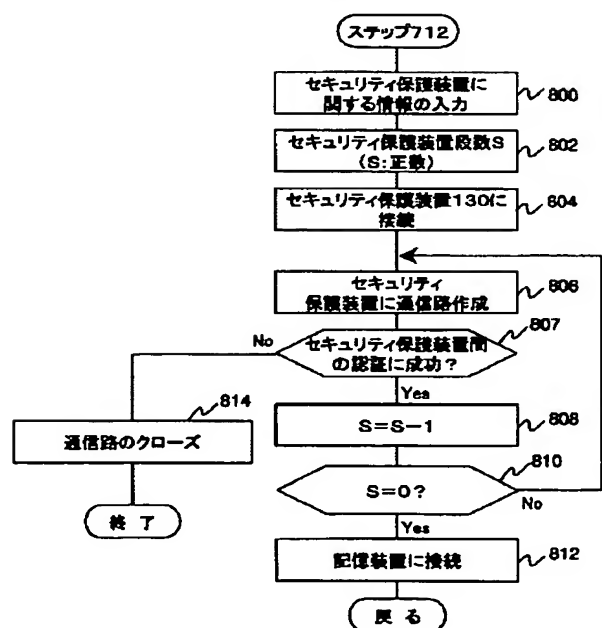
【図7】

図7



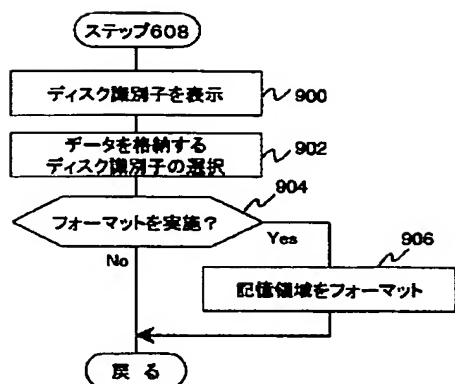
【図8】

図8



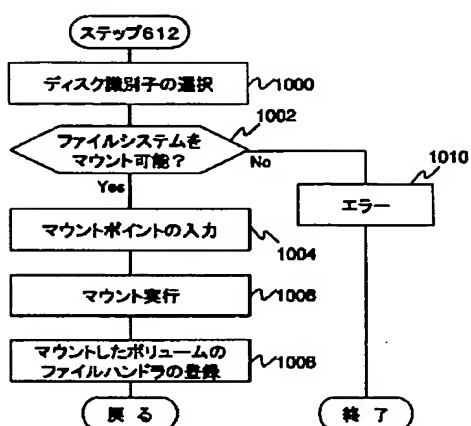
【図9】

図9



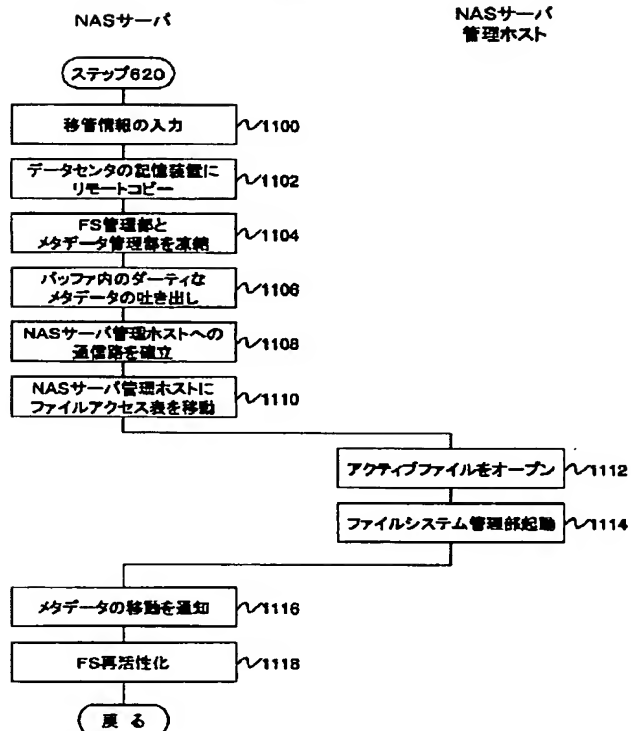
【図10】

図10



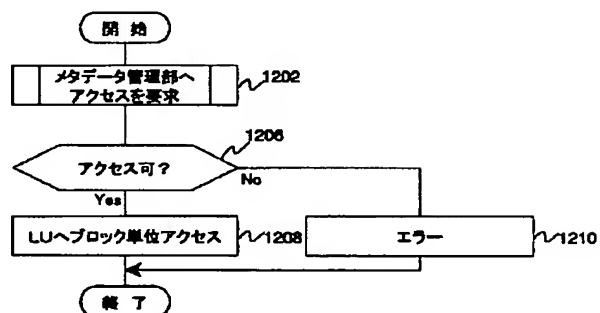
【図11】

図11



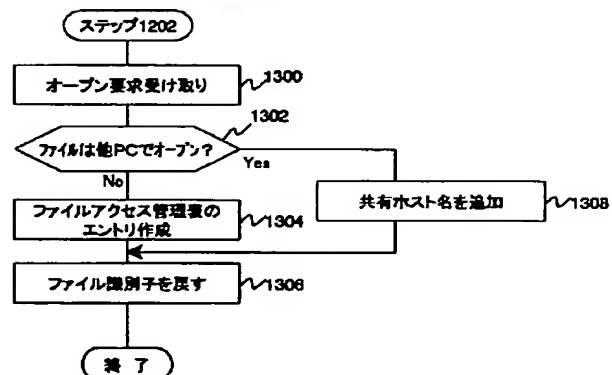
【図12】

図12



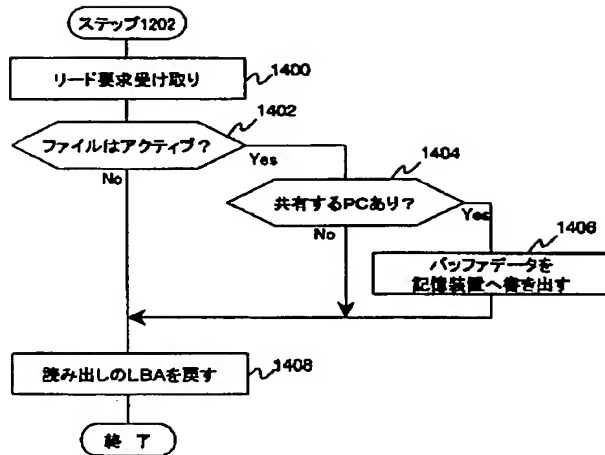
【図13】

図13



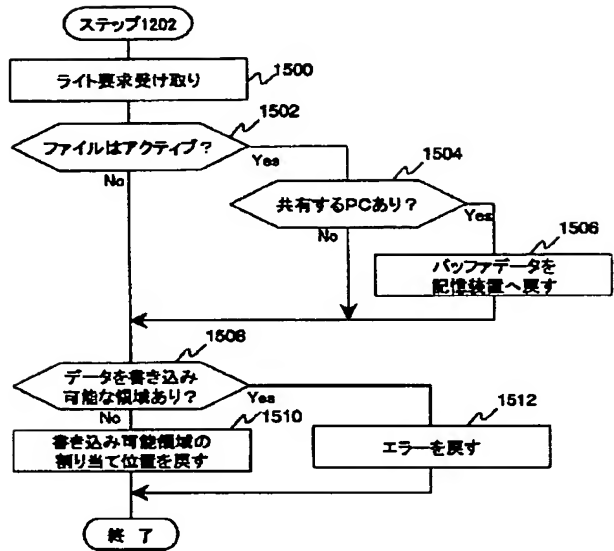
【図14】

図14



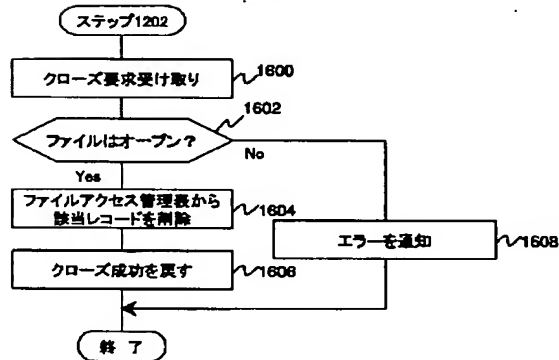
【図15】

図15



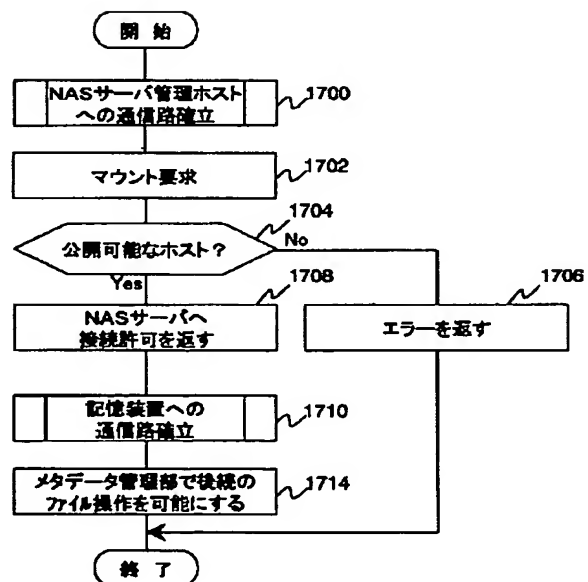
【図16】

図16



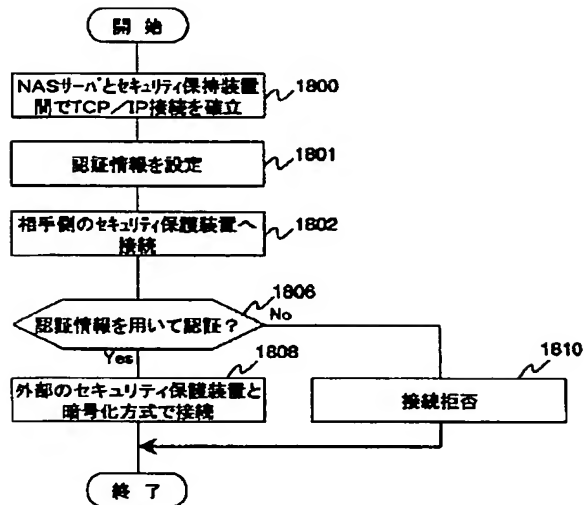
【図17】

図17



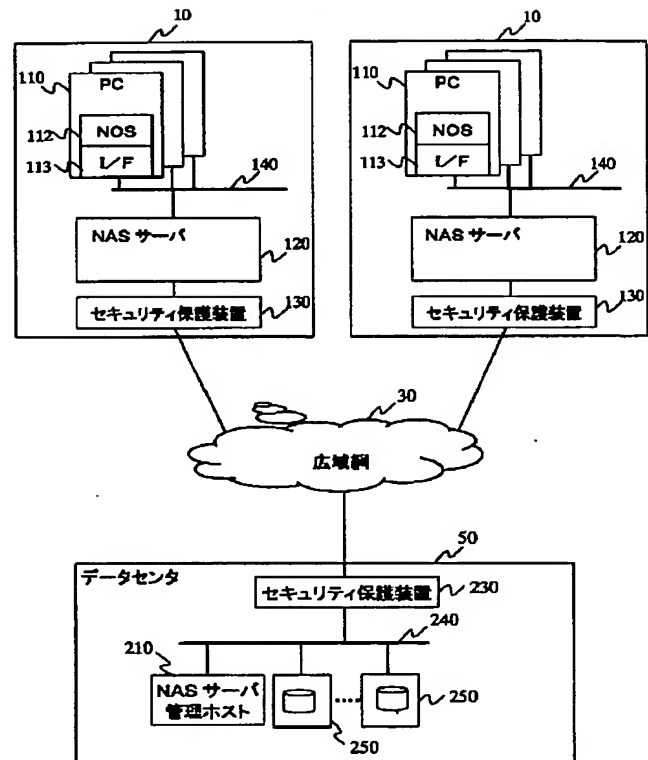
【図18】

図18



【図19】

図19



フロントページの続き

(72)発明者 岩村 卓成
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 ▲高▼本 賢一
神奈川県小田原市中里332番地2号 株式会社日立製作所 R A I D システム事業部内
Fターム(参考) 5B065 BA01 PA04 PA13
5B082 FA01 FA16
5B089 GA12 GA21 GB02 HA01 HA10
JA12 JA40 JB22 KA12 KF01

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.